Rail Security Expert Group

Secure Commissioning

24E232
1A
15.07.2025

Modification history

Version	Date	Modification / Description	Editor
1A	15.07.2025	Initial Release published after internal and external (CER/EIM) review	Klas Andren, Jorge Gamelas, Christof Jungo, Oliver Lovric, Richard Poschinger, Nicolas Poyet, Patrick Rozijn

Table of Contents

1 Introduction 5
1.1 Scope 5
1.2 References 5
1.3 Other referenced documents: 5
1.4 Abbreviations 5
1.5 Authors 6
1.6 Applicability and Document Status 7
1.7 Definition of Requirement Types 7
2 Secure Commissioning Process 8
2.2 Prerequisites 9
2.2.1 Standardised Process 9
2.2.2 Operational Procedures 10
2.2.3 Variants for Technical Implementation 11
2.3 Supplier certificate-based NAC 11
2.3.1 Standardised Process 11
2.3.2 Operational Procedures 11
2.3.3 Variants for Technical Implementation 11
2.4 Issuing an Operator Device Certificate 12
2.4.1 Standardised Process 12
2.4.2 Operational Procedures 12
2.4.3 Variants for Technical Implementation 12
2.5 Issuing additional operator certificates 13
2.5.1 Standardised Process 13
2.5.2 Operational Procedures 13
2.5.3 Variants for Technical Implementation 13
2.6 Operator certificate-based NAC 13
2.6.1 Standardised Process 13
2.6.2 Operational Procedures 14
2.6.3 Variants for Technical Implementation 14

Table of Figures

Figure 1: Use Cases 8
Figure 2: Trust Anchor Installation Process 9

1 Introduction

1.1 Scope

1.1.1.1 The purpose of this document is to provide an overview of and best practices for the secure commissioning process implemented in components built according to the EU-Rail Secure Component Specification [1] and the Shared CyberSecurity Services Specification [2]. Upcoming error corrections (status of June 2025) for an update of these specifications are already presented in this guideline.

1.2 References

1.2.1.1 Subsets and EUG publication are referenced directly with their corresponding ID.

1.3 Other referenced documents:

[1] EU-Rail SP (Cyber) Security Group, „Secure Component Specification BL1.00,“ Europe's Rail Joint Undertaking (EU-Rail), 2025.

[2] EU-Rail SP (Cyber) Security Group, „Shared CyberSecurity Services Specification BL1.00,“ Europe's Rail Joint Undertaking (EU-Rail), 2025.

[3] “RFC 2119,” 1997. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc2119.

1.4 Abbreviations

EU-Rail Abbreviations are listed in the corresponding referenced documents.

1.5 Authors

1.5.1.1 The Rail Security Expert Group (RSEG) consists of security experts of the following groups:

- ERTMS Security Expert Group (ESCG) – Part of the EEIG ERTMS Users Group
- EULYNX Security Cluster – Part of the EULYNX Initiative

1.5.1.2 The following members of the Rail Security Expert Group were involved in creating this document:

- ERTMS User Group (EUG) / EULYNX
  - Richard Poschinger
- NS
  - Patrick Rozijn
- SNCF
  - Nicolas Poyet
- SBB
  - Oliver Lovric
  - Christof Jungo
- Trafikverket
  - Jorge Gamelas
  - Klas Andrén

1.6 Applicability and Document Status

1.6.1.1 In order to ensure the usability for tender documents, this document uses classifications and requirement keywords. This classification does not imply any binding requirements on EUG members or other stakeholders. The documents will be updated in the future to reflect a changing threat landscape, updated standards, and newly developed security solutions.

1.7 Definition of Requirement Types

1.7.1.1 This document uses key words indicating requirement levels according to RFC 2119 [3]. Each clause in this document is classified as follows:

M	Mandatory	function must be implemented as specified
O	Optional	not mandatory, must be as specified if implemented
I	Informative	included for clarification purposes only
R	Recommendation	included as recommendation

Texts without a tag do not constitute a requirement.

2 Secure Commissioning Process

2.1.1.1 The following chapters explain each step of the secure commissioning process as defined in the EU-Rail Secure Component Specification [1]. **(I)**

2.1.1.2 The following figure shows the use cases implemented in the commissioning process. **(I)**

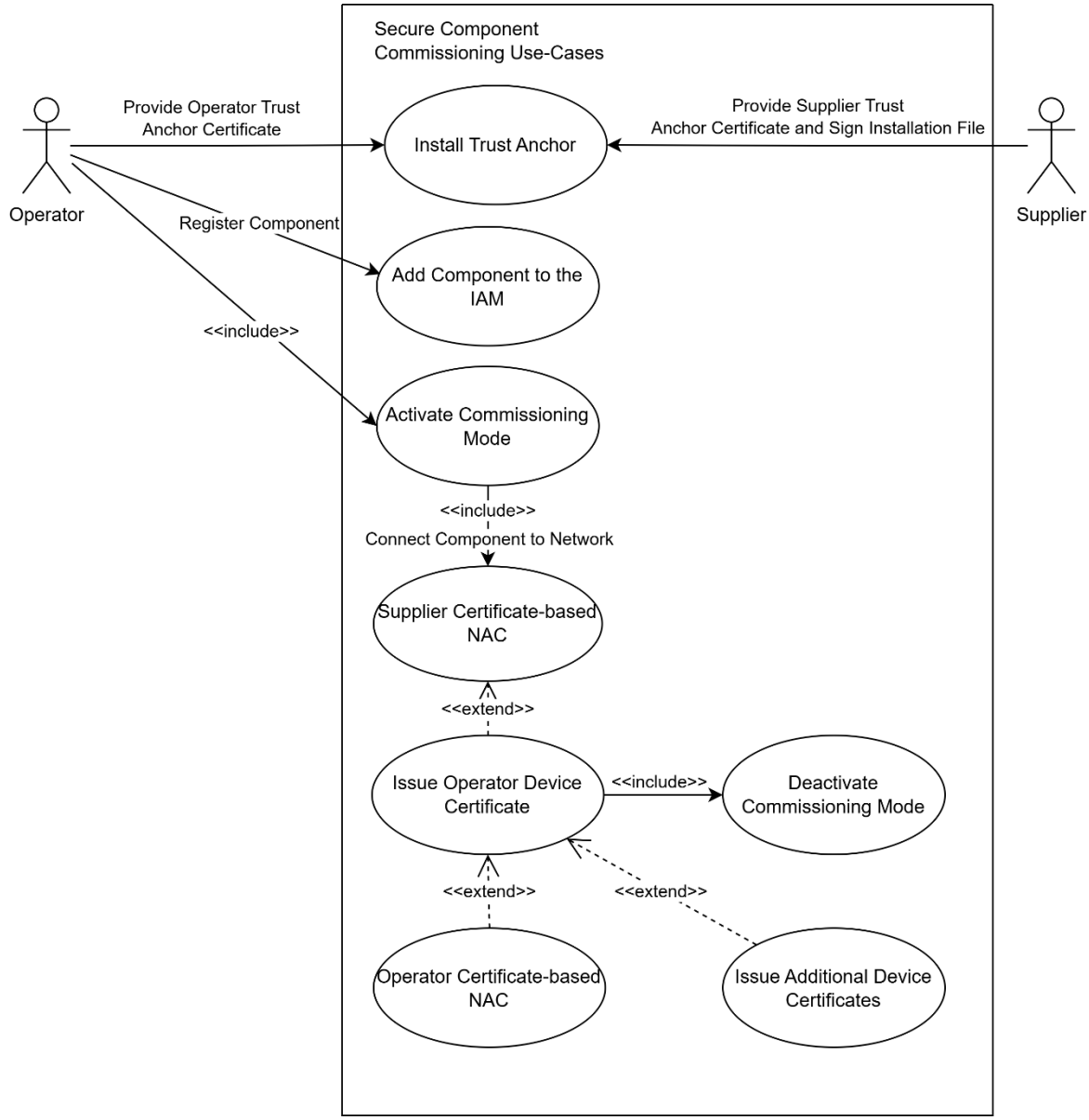

Figure 1: Use Cases

2.1.1.3 In Figure 1 use cases triggered by the operator's and the supplier's personnel are shown. The supplier is responsible for installing its own trust anchor and is involved in installing the operator's trust anchor. The operator is installing its own trust anchor, registering the component in the IAM and activating the commissioning process. Further actions performed are mostly automatically triggered. Actions which can be automatically triggered, or optional procedures are not displayed in this figure, but explained in the following chapters. **(I)**

2.2 Prerequisites

2.2.1 Standardised Process

2.2.1.1 The Supplier provides the Operator with the Supplier Trust Anchor Certificate[1]. Since the Operator uses the Manufacturer Device Certificate (MDC) for the initial network authentication and the initial certificate request, the MDC needs to be validated against the Supplier Trust Anchor Certificate. Consequently, the Supplier Trust Anchor Certificate must be included in the trust store of the PKI-RA and the Network Authentication Server which are responsible for verifying the MDC. **(I)**

2.2.1.2 The Operator adds the Secure Component to the Identity and Access Management. The Identity and Access Management is used to verify that the Secure Component is currently allowed to perform the commissioning process. Using this IAM-based check, network access is granted by the Network Authentication Server and certificate requests are checked by the PKI-RA. In addition, the Supplier Trust Anchor Certificate DN must be added to the appropriate entry in the IAM. **(I)**

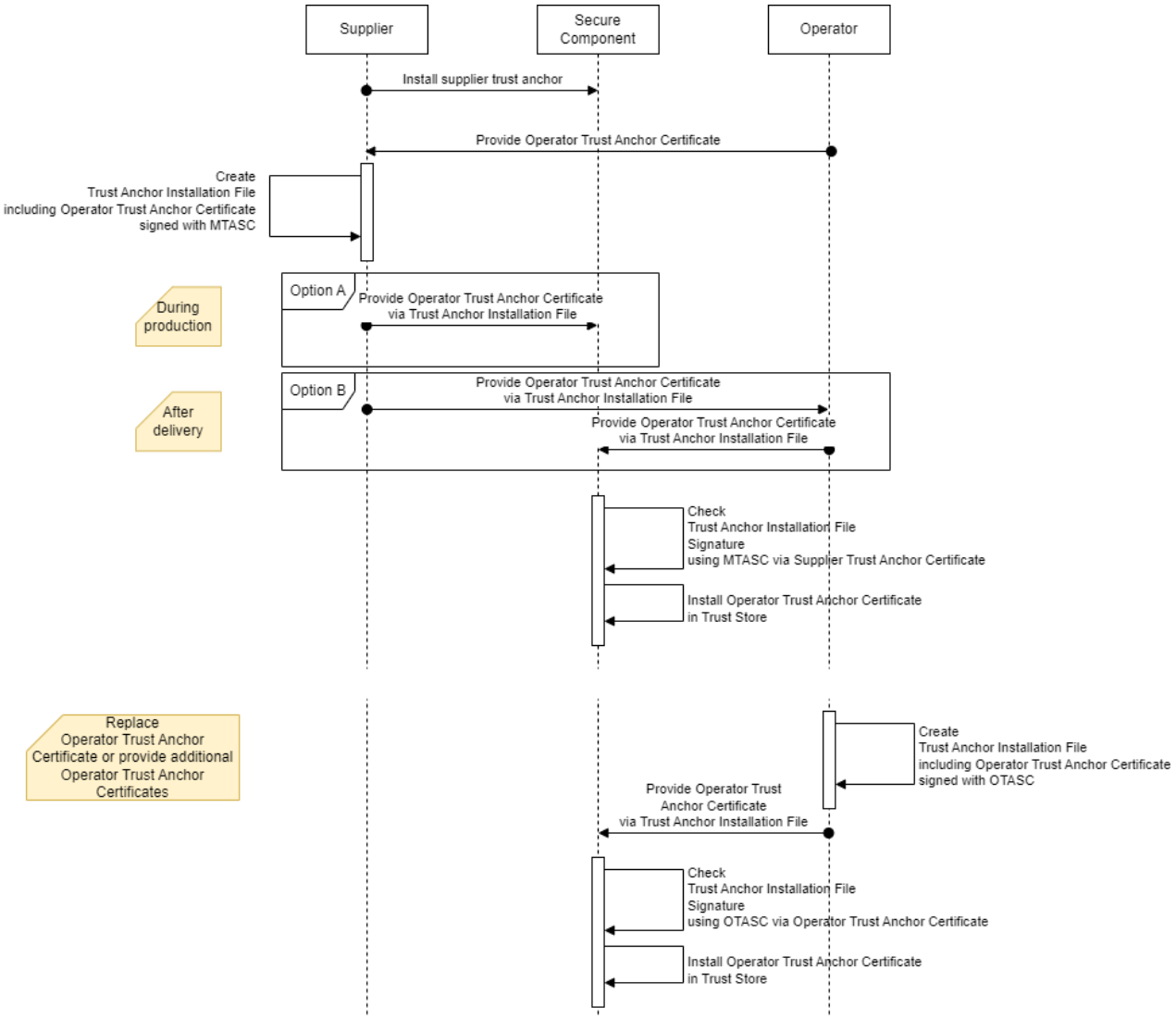

Figure 2: Trust Anchor Installation Process

[1] One or multiple supplier trust anchor certificates

2.2.1.3 The installation of the Operator Trust Anchor Certificate in the Trust Store of the Secure Component can be done by either the Manufacturer or the Operator (see Figure 2). This is required to enable communication establishment, user access and software and configuration verification. The first Operator Trust Anchor Certificate is added to the Secure Component using a Trust Anchor Installation File signed by[2] the Manufacturer Trust Anchor Signer Certificate (MTASC). It can be transferred to the component during the manufacturing process in a proprietary manner. It can also be transferred to the component via an unauthenticated SMI connection in commissioning mode. To add additional Operator Trust Anchor Certificates or replace an Operator Trust Anchor Certificate, the Operator Trust Anchor Signer Certificate (OTASC) can be used to sign the Trust Anchor Installation File. **(I)**

2.2.2 Operational Procedures

2.2.2.1 A Certificate Policy Statement (CPS) that outlines the rules, procedures, and practices for issuing, managing, and using digital certificates in a Public Key Infrastructure (PKI) system is assumed to be available. It defines the specific requirements for certificates and the security measures necessary to ensure the trustworthiness of the PKI system. **(I)**

2.2.2.2 The Operator and the Supplier shall establish a secure process to exchange corresponding Trust Anchor Certificates. **(M)**

2.2.2.3 The following steps provide an example of a secure exchange of Trust Anchor Certificates: **(I)**

- Operator and Supplier must each define at least two trusted employees who are authorized to exchange Trust Anchor Certificates with the other party. These employees must have passed the highest applicable level of background checks available within in the organisation.
- Operator and Supplier must define identification methods for the selected employees. (e.g. ID card or passport)
- These definitions need to be included in relevant agreements and contracts.
- The exchange must take place in person at one of the companies' locations.
- The Trust Anchor Certificates must have their integrity verified using a hash. The hash value must be exchanged via some other means of transport. (e.g. email prior to initiating the exchange).

2.2.2.4 The Operator shall establish a secure communication (e.g. S/MIME encrypted and signed emails or a secure share) with the Supplier to receive serial numbers. **(M)**

2.2.2.5 The Operator shall add the appropriate entities (Secure Component), including serial numbers, to the IAM without granting access rights for NAC via MDC. (Set state in SCS-IAM to "CREATED") **(M)**

2.2.2.6 During the period between delivery and commissioning of a Secure Component, network access based on the MDC should not be possible. It should only be granted when the commissioning process is initiated. **(R)**

[2] Signed by the corresponding private key of the certificate mentioned

2.2.3 Variants for Technical Implementation

- Intentionally left blank -

2.3 Supplier certificate-based NAC

2.3.1 Standardised Process

2.3.1.1 The commissioning process figure used in the EU-Rail Secure Component Specification shows the Secure Component communicating directly with the Network Authentication Server. This is a simplified view, as the Secure Component itself only connects to the Access Switch. The Access Switch is connected to the NAC service. This is detailed in the description of the NAC service in the EU-Rail Shared CyberSecurity Services Specification [2]. **(I)**

2.3.1.2 The Secure Component authenticates to the Access Switch using IEEE 802.1x-2020 with EAP-TLS. For initial authentication it uses the MDC in the commissioning stage. **(I)**

2.3.1.3 The commissioning stage can be identified by the Secure Component e.g. by missing operator certificates and/or missing configuration. In addition, initial configuration data such as IP addresses of the SCS-PKI RA or the Config/SW Repository are provided to the Secure Component e.g. in EULYNX via the Basic Data Identifier (BDI). **(I)**

2.3.1.4 The Access Switch forwards the corresponding data via RADIUS to the SCS-NAC. **(I)**

2.3.1.5 The SCS-NAC verifies the validity of the MDC and requests the SCS-IAM to verify the serial number. The SCS-IAM verifies that an entity corresponding to the serial number is available and set to “COMMISSIONING” state. **(I)**

2.3.1.6 If the access is granted according to the communication chain described above, the Secure Component can access the network. Optionally the operator may decide to implement a separate commissioning network for access based on the MDC. This network only needs to provide access to the SCS-PKI during the commissioning process. This reduces the risk of exposing other services (e.g. EIL, RBC, other SCS) based on an MDC-based authentication. **(I)**

2.3.2 Operational Procedures

2.3.2.1 The Operator shall set the corresponding entity (Secure Component) in the SCS-IAM to “COMMISSIONING” state. **(M)**

2.3.2.2 The Operator shall activate the commissioning procedure of the Secure Component. **(M)**

2.3.2.3 Depending on the type of Secure Component, the commissioning procedure is automatically activated, if no ODC is available on the component. **(I)**

2.3.2.4 When the commissioning procedure has been successfully completed, the Operator shall deactivate the commissioning state for the corresponding entity (Secure Component) in the SCS-IAM. (Set state to “ACTIVE”) **(M)**

2.3.3 Variants for Technical Implementation

2.3.3.1 The Operator should implement a virtually separate commissioning network that only allows access to SCS-STS and SCS-PKI via authentication using the MDC. **(R)**

2.3.3.2 Implementing a separate commissioning network might require network capabilities not provided by standards (e.g. EULYNX) which integrate the EU-Rail Cybersecurity Specifications. **(I)**

2.3.3.3 The SCS-IAM should automatically deactivate the commissioning mode. (Set state to “ACTIVE”) **(R)**

2.3.3.4 The automatic deactivation of the commissioning mode in the SCS-IAM can be triggered internally depending on the certificate’s information added to the SCS-IAM or by another SCS (e.g. SCS-PKI after all certificates have been issued). **(I)**

2.4 Issuing an Operator Device Certificate

2.4.1 Standardised Process

2.4.1.1 After SCS-NAC has granted access to the network, the Secure Component can start the process of obtaining an Operator Device Certificate (ODC). **(I)**

2.4.1.2 The Secure Component generates the private/public key pair for the ODC and creates the CMP initialization request with the required information according to the corresponding certificate profile. **(I)**

2.4.1.3 The Secure Component sends the Initialization Request message to the SCS-PKI RA via SSI-PKI. The initialization request uses message protection provided by the MDC. **(I)**

2.4.1.4 SCS-PKI RA verifies message protection using the Supplier Trust Anchor Certificate and also verifies with the SCS-IAM that the corresponding entity exists and it is in “COMMISSIONING” state via the SSI-IAM. This step may include a metadata check performed by the operator, which is discussed further in Chapter 2.4.3. **(I)**

2.4.1.5 If both checks are successful, the SCS-PKI RA can forward the Initialization Request message to the ECS-PKI CA. ECS-PKI CA signs and creates the appropriate certificate using the appropriate Operator Trust Anchor Certificate. **(I)**

2.4.1.6 After the SCS-PKI RA forwards the initialization response to the Secure Component, the Secure Component installs the ODC and confirms the received ODC with the Certificate Confirmation message. This is also confirmed by the SCS-PKI RA using the PKI Confirmation message. **(I)**

2.4.2 Operational Procedures

2.4.2.1 The issuing of the ODC is triggered automatically without the need for any further Operator interaction. **(I)**

2.4.3 Variants for Technical Implementation

2.4.3.1 The standardized process for issuing the ODC (and other operator certificates) results in certificates being signed based solely on the trust in the MDC. The remaining risk is reduced by only allowing network access and responding to certificate requests, based on the “COMMISSIONING” state stored in the SCS-IAM. Highly coordinated attacks may still be able to circumvent these measures. Therefore, additional risk mitigation can be implemented using the optional metadata check. **(I)**

2.4.3.2 The metadata check allows the operator (e.g. field technician) to confirm the issuing of the ODC upon receipt of the CMP certificate request by the ECS-PKI RA. The following metadata of the incoming CMP certificate request should be checked: **(R)**

- Source IP address
- Receival time
- Serial number of MDC

2.5 Issuing additional operator certificates

2.5.1 Standardised Process

2.5.1.1 The Secure Component generates the private/public key pair for all remaining and required Operator certificates. It generates the CMP initialization request with the required information according to the corresponding certificate profile. **(I)**

2.5.1.2 The Secure Component sends the Certification Request message to the SCS-PKI RA via SSI-PKI. The initialization uses the message protection provided by the ODC. **(I)**

2.5.1.3 SCS-PKI RA verifies message protection using the Operator Trust Anchor Certificate. **(I)**

2.5.1.4 If the check passes, the SCS-PKI RA can forward the Certification Request message to the ECS-PKI CA. The ECS-PKI CA signs and creates the appropriate certificate using the appropriate Operator Trust Anchor Certificate. **(I)**

2.5.1.5 After the SCS-PKI RA forwards the Certification Response to the Secure Component, the Secure Component installs the additional Operator certificates and confirms the received certificates with the Certificate Confirmation message. This is also confirmed by the SCS-PKI RA using the PKI Confirmation message. **(I)**

2.5.2 Operational Procedures

2.5.2.1 The issuing of additional Operator certificates is triggered automatically without any further action by the Operator. **(I)**

2.5.3 Variants for Technical Implementation

- Intentionally left blank -

2.6 Operator certificate-based NAC

2.6.1 Standardised Process

2.6.1.1 After the operator certificates are issued and installed, the Secure Component authenticates to the Access Switch by using the ODC and IEEE 802.1x-2020 with EAP-TLS. The reauthentication can be started by triggering link down and then back up. **(I)**

2.6.1.2 The Access Switch forwards the appropriate data via RADIUS to the SCS-NAC. **(I)**

2.6.1.3 The SCS-NAC verifies the validity of the ODC and requests the SCS-IAM to verify the Common Name. The SCS-IAM verifies that an entity corresponding to the Common Name is available and set to “ACTIVE” state. **(I)**

2.6.1.4 When the NAC access has been granted, the Secure Component is granted network access to all required Shared Cybersecurity Services, Other OT Services (e.g. MDM) and

other connected Secure Components (e.g. EULYNX Light Signal Controller is granted access to Electronic Interlocking). **(I)**

2.6.2 Operational Procedures

2.6.2.1 Access to the network via NAC is granted automatically without any further interaction by the operator. **(I)**

2.6.3 Variants for Technical Implementation

- Intentionally left blank -